D1

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-285283A**

(43)Date of publication of application : **12.10.2001**

(51)Int.Cl. **H04L 9/32**
G09C 1/00
H04L 9/08
H04L 12/28
H04L 12/66

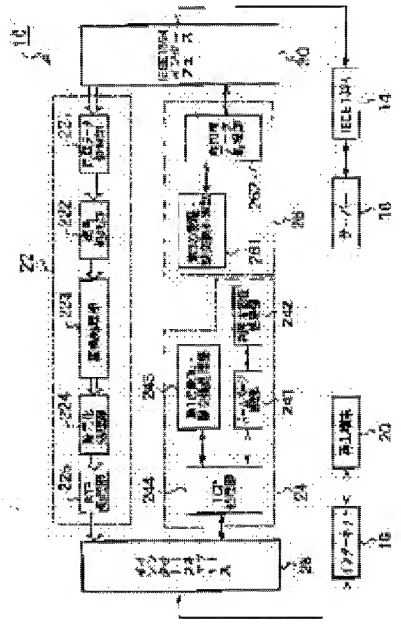
(21)Application number : **2000-094840**

(22)Date of filing : **30.03.2000**

(71)Applicant : **TOSHIBA CORP**

(72)Inventor : **SAITO TAKESHI**

(54) COMMUNICATION UNIT AND ITS COMMUNICATION METHOD



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a communication unit that can realize protection of copyright in the case of transmitting data from a home network to a public network and to provide its communication method.

SOLUTION: The communication unit interconnects a public network 16 such as the Internet and a home network 14 such as a network in compliance with the IEEE 1394. This communication unit consists of a 1st authentication/key exchange processing section 243 that performs authentication/key exchange with a reproduction terminal 20 connected to the public network 16, a 2nd authentication/key exchange processing section 261 that performs authentication/ key exchange with a server 18 connected to the home network 14, a transmission section 22 that transmits AV data that are encrypted for copyright protection and obtained from the server 18 to the reproduction terminal 20, and a user authentication processing section 242 that authenticates a user of the reproduction terminal 20 and rejects communication with the reproduction terminal 20 when the user cannot be authenticated.

Detailed Descriptions of the Invention:

.....

[0014] Fig. 1 is a block diagram illustrating an overall configuration of a network system provided with a communication unit according to an embodiment of the present invention. As illustrated in Fig. 1, a communication unit 10 according to the embodiment of the present invention is connected between a home network 14 installed in a home 12 and configured using IEEE1394 or the like and a public network 16 provided outside the home 12 and configured of the Internet or the like. The home network 14 is connected with a server 18 storing various types of AV data. The AV data stored in the server 18 is transmitted from the home network 14 to the public network 16 through the communication unit 10. The public network 16 is connected with a reproduction terminal 20 capable of reproducing AV data. The reproduction terminal 20 receives the AV data transmitted from the communication unit 10 through the public network 16. Then, the reproduction terminal 20 reproduces the received AV data.

.....

[0037] (11) In step S112 in Fig. 3, the communication unit 10 encrypts the AV data converted into MPEG-4 symbol again using a second encryption key K2 (step S212 in Fig. 5). The AV data is a content having encryption control information "No More Copy" originally written therein. That is to say, copy or recording prohibited data should be transmitted in such a form as to allow prevention of recording and copying also in retransmission of such data. Thus, even after being changed, the AV data has "No More Copy" written therein. The reason that such re-encryption is executed after steps S102 to S105 in Fig. 3 is that a user of the reproduction terminal 20 is much anticipated to be a proper user based on first input of a password and thus it becomes obvious that subsequent procedures are the ones for private enjoyment of the user.

[0038] (12) In step S113 in Fig. 3, the communication unit 10 transmits re-encrypted AV data (MPEG-4 data) to the reproduction terminal 20 through the Internet 16 (step S213 in Fig. 5). RTP is utilized as a transfer protocol. Besides, the re-encrypted AV data has encryption control information "No More Copy" written therein, as described above. This prevents the received AV data from being improperly accumulated by the reproduction terminal 20.

[0039] (13) In step S114 in Fig. 3, the reproduction terminal 20 which receives the re-encrypted AV data (MPEG-4 data) recognizes that authentication and key exchange are required from the fact that the AV data are encrypted. Then, the reproduction terminal 20 executes authentication and key exchange with the communication unit 10. The authentication and key exchange allow the reproduction terminal 20 to acquire a second decryption key required for decryption of the re-encrypted AV data. For example, when an encryption technique to be utilized is a common key encryption, the second decryption key is the same as the second encryption key K2. Communication between the reproduction terminal 20 and the communication unit 10 is executed in a form of a TCP packet, for example.

[0040] Here, it is preferable that the communication unit 10, upon reception of a request for authentication and key exchange from the reproduction terminal 20 (step S215 in Fig. 5), verifies whether or not a user of the reproduction terminal 20 is a person who is determined to be a proper

user through the user authentication in steps S102 to S105 in Fig. 3 (step S215 in Fig. 5). This is because contents may be transmitted to an indefinite number of persons through the Internet 16 if the user is not a proper user, which is against a principle that "time shift, processing or the like are allowed for only personal use". Step S215 in Fig. 5 allows such a trouble to be prevented in advance. When the user is improper (NO in step S215 in Fig. 5), the communication unit 10 immediately cuts off a link connected to the reproduction terminal 20 (step S204 in Fig. 5).

[0041] In this way, the reproduction terminal 20 of a proper user allows acquirement of the second decryption key K2 without being known to others, thereby to decrypt the received re-encrypted AV data. As described above, however, as the AV data has "No More Copy" written therein, the reproduction terminal 20 cannot accumulate/copy the AV data. The reproduction terminal 20 can only decode/display the AV data at that time.

[0042] As described above, in transmitting AV data including a channel crop or of a work itself acquired on a home network to a public network, the embodiment of the present invention provides secure protection for a work under the copyright law.

.....

FIG.1

10 COMMUNICATION UNIT

14 HOME NETWORK

16 PUBLIC NETWORK

18 SERVER

20 REPRODUCTION TERMINAL

HOME

.....

FIG. 3

20 REPRODUCTION TERMINAL

16 INTERNET

10 COMMUNICATION UNIT

14 IEEE1394 BUS

18 SERVER

S101 HOME PAGE REQUEST

S102 USER ID AND PASSWORD REQUEST

S103 USER ID AND PASSWORD

S104 VERIFICATION

S105 HOME PAGE

S106 CONTENT REQUEST

S107 CONTENT TRANSMISSION REQUEST

S108 ENCRYPTED AV DATA (MPEG-2 DATA)

S109, S114 AUTHENTICATION AND KEY EXCHANGE

S110 DECRYPTION

S111 CONVERSION

S112 ENCRYPTION

S113 ENCRYPTED AV DATA (MPEG-4 DATA)

.....